

CLAIMS

What is claimed is:

1. A high speed add rotate add system, comprising:
 - a first rotator operable to receive a first input and a shift control signal for rotating
5 the first input;
 - a carry save adder operable to receive a second input, a third input and the rotated first input, the carry save adder operable to sum the second input, third input and rotated first input, and to output a sum and carry output;
 - a shift decoder operable to receive the shift control signal and output a carry
10 control signal; and
 - a carry select propagating adder operable to receive the sum and carry outputs from the carry save adder and the carry control signal from the shift decoder, the carry select propagating adder operable to manipulate data contained within the sum and carry outputs based upon the carry control signal from the shift decoder and to output a result
15 coincident with a summation of the first, second and third inputs.
2. The system of claim 1, the first, second and third inputs have a bit length of X, where X is a positive integer.
- 20 3. The system of claim 2, wherein the carry save adder comprises a plurality of full adders, wherein respective full adders are operable to sum corresponding bits of the second input, third input and rotated first input.
4. The system of claim 3, wherein the carry save adder comprises X number
25 of full adders.
5. The system of claim 2, wherein the carry select propagating adder comprises a plurality of full adders.
- 30 6. The system of claim 5, wherein the carry select propagating adder comprises X number of full adders.

SE0033

7. The system of claim 1, wherein the carry select propagating adder comprises carry generation logic that is operable to receive the carry control signal from the shift decoder and to adjust the output of the carry select propagating adder based upon the carry control signal.

8. The system of claim 7, wherein a bit of the output of the carry select propagating adder is assigned a zero if a corresponding bit of the carry control signal is zero.

9. The system of claim 1, wherein the shift control signal is based upon $\log_2 X$, where X is a positive integer.

10. The system of claim 9, wherein the shift decoder operates according to
for $(i=1; i < X; i=i+1)$
carry control signal[i] = $\sim (i == \text{shift control signal})$.

11. The system of claim 1, wherein a path from the first input to the first rotator to the carry save adder to the carry select propagating adder and out through the second rotator is a critical path.

12. The system of claim 1, wherein the sum output corresponds to an exclusive OR operation performed on three one bit inputs.

13. The system of claim 1, wherein the carry output corresponds to an OR operation performed on respective results from three AND operations performed on three possible two input combinations for three one bit inputs.

14. The system of claim 1, wherein the carry save adder performs according to the following truth table:

SE0033

first input	second input	third input	carry	Sum
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

15. The system of claim 1, wherein the add rotate add operation is implemented in performing an HMAC-MD5-96 algorithm.

5 16. The system of claim 1, wherein the add rotate add operation is implemented in an IPsec module.

17. The system of claim 1, wherein the add rotate add operation is implemented in an RX IPsec processor.

10

18. The system of claim 1, wherein the add rotate add operation is implemented in an TX IPsec processor.

15 19. The system of claim 7, wherein a bit of the carry output is assigned a zero if a corresponding bit of the carry control signal is zero.

20. The system of claim 1, wherein the carry select propagating adder operates according to:

20 $P[i] = A[i] \text{ XOR } B[i]$
 $G[i] = A[i] \text{ AND } B[i]$
 $S[i] = P[i] \text{ XOR } C[i]$
 $C[i+1] = G[i] \text{ OR } C[i] \text{ AND } P[i]$
and
 $C[0] = C[4]'$
25 $C[1] = CS[1] \text{ AND } C[1]'$

SE0033

$$C[2] = CS[2] \text{ AND } C[2]'$$

$$C[3] = CS[3] \text{ AND } C[3]'$$

and

$$C[1]' = G[0] \text{ OR } P[0] \text{ AND } C[4]'$$

5 $C[2]' = G[1] \text{ OR } P[1] \text{ AND } C[1]' = G[1] + P[1]G[0] + P[1]P[0]C[0]'$

$$C[3]' = G[2] \text{ OR } P[2] \text{ AND } C[2]' =$$

$$G[2] + P[2]G[1] + P[2]P[1]G[0] + P[2]P[1]P[0]C[0]'$$

$$C[4]' = G[3] \text{ OR } P[3] \text{ AND } C[3]' =$$

$$G[3] + P[3]G[2] + P[3]P[2]G[1] + P[3]P[2]P[1]G[0] + P[3]P[2]P[1]P[0]C[0]'$$

10

21. A method of performing a fast add rotate add operation, comprising:
performing a rotation operation on a first input according to a shift control signal;
adding the rotated first input, a second input and a third input to obtain a sum and

a carry;

15 decoding a carry control signal from the shift control signal; and
adjusting the carry based upon the carry control signal.

22. The method of claim 21, wherein at least one of: the first, second and third
inputs have a bit length of X and the shift control signal is based upon $\log_2 X$, where X is
20 a positive integer.